Finding & Restrain uncontrolled Data and Forensics Analysis

Arunreddy Pothireddy

Asst.Prof, Department of Computer Science & Engineering
Christu Jyothi Institute of Technology & Science, Andhrapradesh, India.

Abstract: Growing volumes of data has to be protected by organizations; exfilteration has become an increasing concern. This paper is intended to focus on the procedural artifacts that should be considered when facing exfilteration incident Analyzing, detecting & Deterring of Data.

I. Introduction

In today's world, an organization's digital resources are likely to be among its most sensitive and valuable assets. If a competitor were to obtain details of research and development, financial information, business processes, or intended developments and acquisitions, it could prove commercially disastrous. Hence foreign nations are investing huge amounts in state-supported cyber attacks to obtain these assets for use by organizations within their own countries. The attacks are almost always successful. Modern organizations are so large, diverse and complicated that they are frequently unaware of what sensitive documents they possess, let alone how to defend them appropriately. Furthermore, an organization's network perimeters will be highly porous and susceptible to attack via a host of new technologies, such as remote access, cloud services, home working, partnerships and so on. The internal networks of modern organizations are also complex and interlinked, having grown from principles of usability rather than security, which mean that it can prove extremely difficult to detect attackers once they are within the network. This is partly because detection methods often focus on spotting 'bad' patterns of behavior, so that attackers can avoid detection simply by restricting themselves to 'good' patterns – such as accessing the CEO's email from the CEO's own laptop.

Data can have real value to attackers, potentially in the region of millions or even billions of pounds where intellectual property and negotiation positions are concerned. Attacker motivation and resourcing, combined with modern networks that are highly complex and porous, mean that it is simply not possible to guarantee the prevention of data exfiltration. If necessary, attackers can spend years slowly mapping out an organization, observing legitimate behavior to avoid tripping defenses and gradually working towards their objectives. If they come up against defenses, the attackers can either learn to bypass the controls directly, or compromise the company that produces a control in order to bypass it.

However, organizations can significantly increase the number of opportunities they have to detect and repel attackers. In so doing, they can escalate the cost and complexity for the attacker, reduce the potential business impact on themselves, and even develop advanced strategies that will deter the attacker from targeting them in future. This white paper gives a high-level overview of a typical attack (see section on 'Anatomy of a Typical Attack') and then covers the current tactics used by attackers to acquire and exfiltrate data (section 'Current ExfltratioTactics'). Current business trends and attacker trends are then extrapolated to predict the likely future developments in exfiltration strategy (section 'Future Exfiltration Tactics'). The majority of the white paper, however, focuses on the steps that will give organizations the best chance of detecting and deterring data exfiltration (section 'Increasing Organizational Resilience'), before concluding with a summary. The appendices contain a glossary of terms, recommended further reading, and a list of 'quick wins' that can increase an organization's resilience while a more comprehensive defense program is being developed.

II. Identification of Data

Once a network has been compromised and the C&C infrastructure set up, attackers will need to seek out the data that is useful to them. This is rarely data that relates solely to a specific project, but will more usually be wider information relating to the organization, its structure, network topologies, connections to the outside world – and its defenses. CPNI has produced comprehensive advice under the title 'Protecting Information About Networks, the Organization and its Systems (PIANOS)'. To identify information of interest, some attackers will simply list the machines on the domain and then mount the flee shares of machines that sound relevant from their hostname or description. Attackers then browse the flee shares for folders or documents of potential interest. More advanced attackers, or attackers who have no success with browsing flees, will attempt more targeted identification of information using resources such as wikis and Share Points. Typically, a great deal of information useful to an attacker is available with low privilege credentials, as details of individuals and organizational structure are usually available to all employees on internal portals or document management systems. Once the individuals with access to the required documents have been identified, attackers will be able to focus on horizontal and vertical movement throughout the network to obtain the remainder of the information they seek. Attackers will use a variety of techniques to move through the network, including key logging, privilege escalation exploits and password dumping and cracking.

III. Exfiltration Channels

Controls currently used by most organizations do not prevent simple exfiltration channels and hence attackers are relatively unrestrained when it comes to their exfiltration method. Attackers therefore tend to use simple, reliable, overt, high-bandwidth methods, typically the protocols by which any technical user is likely to transfer a large flee.

C&C Channel: During a compromise, attackers will typically install C&C malware from which to attack the internal network. The malware communicates with the attacker's supporting infrastructure, allowing external control. Different C&C tools use different methods to communicate and attackers will often use the C&C channel to exfiltrate data, as they know the connection works and has not been prevented by the organization's defenses. However, C&C channels tend to be used only for small volumes of flees, as higher-bandwidth methods are often available for large flee archives. CPNI has produced separate guidance regarding the detection of C&C channels.

HTTP/S: A common method for uploading flees is transfer over HTTP or HTTPS. This is a reliable protocol that enables large flee transfers and has the added benefit that it is probably allowed through a web proxy, even if direct outbound connections are prohibited. Many C&C tools use HTTP and HTTPS as a communications channel, however, some have been observed that do not, and yet still use HTTP uploads to exfiltrate flees. HTTPS has the additional benefit (for the attacker) that unless organizations are using SSL interception (and the attacker's tool accepts the intercepting certificate), investigators will not be able to determine what was being exfiltrate from network packet captures.

Email: The vast majority of organizations allow email (SMTP traffic) to arbitrary addresses, even when other outbound connections are prevented, and so attackers will sometimes exfiltrate flees by this method. Exfiltration by email does not typically require the attacker to supply tools, as the majority of systems that might be compromised will already have the necessary tools. However, many organizations limit the size and nature of attachments, hence attackers will often send the data, obfuscated or encrypted, in many small chunks. Tools are likely to be required to prepare the data appropriately for exfiltration. Alternatively, attackers can use third-party cloud email services (see below) to bypass restrictions put in place by the organization's mail servers.

IV. Exfiltration Tactics

Currently, attackers are not forced to use particularly advanced techniques, as few organizations beyond government departments dealing with highly classified material have controls in place that detect and deter even basic exfiltration. However, as organizations become more security-aware, attackers will need to use more sophisticated techniques to exfiltrate data. Current trends suggest that attackers will increasingly utilize services via which organizations allow (or even require) outbound traffic. In this way, attackers will attempt to 'hide in the noise' by using channels that are also used legitimately, making it harder to detect at the perimeter. Such services will typically have a large bandwidth for data exfiltration. For particularly hardened targets, attackers might instead use covert or out-of-band channels, which are very difficult to detect but typically have much lower bandwidth than overt techniques. Hence they tend to be useful only for stealing documents of particular interest, rather than entire data sets. The controls described in the 'Increasing Organizational Resilience' section will help an organization to detect or deter attackers regardless of the exfiltration methods used; however, some business trends, such as increased storage of data in third-party Clouds and hosted services can reduce the effectiveness of those controls and that will need to be factored into risk decisions.

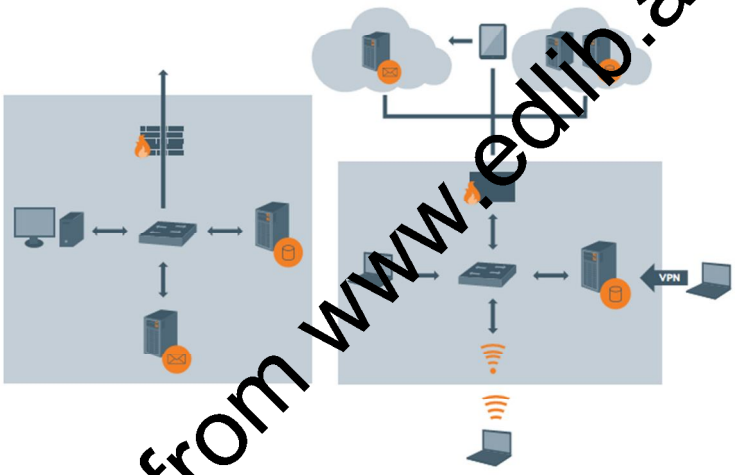

Fig: Modern networks are complex and porous, with cloud services, mobile workers, smart phones etc.

Changes to Data Aggregation and Preparation: As defensive controls improve, attackers are likely to change their tactics to evade defensive measures. Organizations can expect to see greater abuse of legitimate functionality, as well as greater care taken by attackers when using a targeted account for certain behaviors, in an attempt to avoid detection due to inappropriate access. For example, an attacker dumping the CEO's email to the CEO's laptop will look less suspicious than if the mailbox were dumped to a normal workstation. Alternatively, attackers might attempt to recover the mailbox from the laptop itself, rather than from the mail server. As many organizations move to service-oriented architectures (SOA), where data is exposed through web services, it may be that attackers start to use these interfaces to gather the data, rather than via traditional views such as websites or GUIs. There are indications that attackers are already starting to use forensics tools – for example, flee carving utilities – to recover deleted (but not securely erased) flees. These earlier versions of flees can be useful to attackers, particularly if they contain data that was later redacted or classified and deleted. Advanced attackers have already been seen using forensics tools to hide data when aggregating it prior to exfiltration. Attackers are likely to use locations such as Volume Shadow Copy, unused disk space and alternate data streams (ADS), so that investigators examining a machine that appears to be aggregating do not locate the flees being prepared for exfiltration.

Exfiltration by Popular Websites: There are many websites that now form a regular part of people's lives. There is therefore significant pressure, verging on demand, to use those services at work. Many people use

social networks throughout the day and, if staff is prevented from doing so, it could cause problems. However, In particular, where images and videos can be uploaded, it is possible to exfiltrate far larger volumes of information – via data encoded within an image flee – than as raw text. Indeed, experiments conducted on major social networks have demonstrated that it is possible to exfiltrate up to 20GB of data in a single flee in this way (see box-out). If attackers move to exfiltration data through popular websites, it will require a change to controls at the perimeter, since it will be difficult to blacklist or even monitor volumes of traffic when there are often legitimate reasons for large data uploads (for example, an employee uploading holiday photos to a photo-sharing site). However, the remainder of the controls described in the 'Increasing Organizational Resilience' section provides multiple opportunities to detect and deter attackers before they can exfiltrate data using such websites.

Table: List of Websites providing Exfilteration

WEBSITE	HOW MUCH DATA CAN BE EXFILTRATED
YouTube	20GB as a video
Flickr	200MB as an image, up to 1TB
Vimeo	5GB of videos per week; paid subscription required to retain original file
Facebook	25MB raw file for groups, 1GB as video, unlimited profile, text posts
LinkedIn	100MB Office documents
DeviantArt	60MB as an image, up to 300MB
Pinterest	10MB as an image
Tumblr	10MB as an image, 150 photo posts allowed per day, text posts

V. Case Studies

Misunderstanding the Threat: An organization in the corporate services sector managed its risk based on the perceived primary threat of competitors hoping to gain an advantage, or other insight into their client relationships. As such, the organization believed its primary assets were its financial data and client contacts. An investigation found that it had been compromised by at least one attacker thought to be funded by a nation state – and that the attacker was compromising not the organization's own data but its clients' data. In other words, by holding intimate details of its clients' businesses, the organization had become a target itself.

Exfiltration Can be Easy: Attackers do not always need to exfiltrate data through advanced methods. One organization was compromised by attackers who were primarily after email content. An investigation found that attackers had compromised credentials for the email Accounts of senior members of staff, and then set up email forwarding rules so that a copy of every email received was sent to an account at a cloud provider. This traversed the outbound proxy and was found to have been active for several months.

Exfiltration Can be Advanced: Attackers tend to take the easiest routes available to them, to avoid exposing their more advanced capabilities. However, should it be required, attacker groups have shown that they can call on advanced methods. Examples of this include attackers that have assessed segregated environments for protocols that are permitted to cross the network boundary – and then rewritten their tools to use those protocols. There are also examples where attackers have successfully crossed air gaps, using such techniques as compromising the USB media that the organization's staff was using to transfer

data into an environment. Researchers have also demonstrated proof of concepts that use ultrasound via a device's built-in speakers and microphone to cross an air gap.

No Magic Bullets: Many products exist that claim to prevent advanced attacks and hence organizations can place too much reliance on a particular product, rather than implementing a robust defense-in-depth approach. An example is the 'Hidden Lynx' hacking campaign reported by Symantec. A military contractor in the U.S. was using an application white listing tool by Bit9. This was preventing attackers from running their own tools, so the attackers simply shifted their focus to Bit9 itself – stealing the Bit9 code-signing certificates, which enabled the attackers to sign their tools with Bit9's certificate. Hence they were readily able to run their own tools on systems protected by Bit9.

VI. Conclusion

Modern organizations are highly complex and have valuable digital assets that they need to use in day-to-day business rather than simply store securely. Modern attackers are motivated and well-resourced by groups that understand the value of the assets they hope to compromise. This combination means that complete prevention of data compromise and exfiltration by advanced attackers simply isn't possible. Instead, organizations must focus on detecting and deterring such attacks, which is still a significant challenge. However, if well implemented, such a strategy will be able to push up the cost to the attacker while simultaneously decreasing the business impact on the organization. A coherent strategy can work to flip the defender's dilemma (the idea that an attacker only needs to be successful once) into the attacker's dilemma (where a single detection can alert the defender to their presence).

References

1. Meet Hidden Lynx: The most elite hacker crew you've never heard of' by Dan Goodin on arstechnica http://arstechnica.com/security/2013/09/meet-hidden-lynx-the-most-elite-hacker-crew-youve-never-heard-of/
2. Mandiant Intelligence Center Report 'APT1: Exposing One of China's Cyber Espionage Units' http://intelreport.mandiant.com/
3. 'Advanced Data Exfltration' by Ifatch Ian Amit http://www.iamit.org/blog/2012/01/advanced-data-exfltration/
4. SharePoint – Microsoft http://ofce.microsoft.com/en-us/sharepoint-server-help/introduction-control-user-access-with-permissions-HA101794487.aspx
5. Hacking Exposed Wireless by Cache, Wright and Liu Book on wireless security secrets and solutions